[Logo der Organisation]

[Name der Organisation]

RICHTLINIE ZUR ENTWICKLUNGSSICHERHEIT

Code:	
Version:	
Datum der Version:	
Erstellt durch:	
Genehmigt durch:	
Vertraulichkeitsstufe	

Commented [27A1]: Alle mit eckigen Klammern [ ] markierte Felder in diesem Dokument müssen ausgefüllt werden.

Commented [27A2]: Um mehr über dieses Thema zu erfahren, lesen Sie bitte diesen Artikel:

How to integrate ISO 27001 A.14 controls into the system/software development life cycle (SDLC)
https://advisera.com/27001academy/blog/2017/01/24/how-to-integrate-iso-27001-a-14-controls-into-the-system-software-development-life-cycle-sdlc/

Commented [27A3]: Die Systematik für die Kodierung von Dokumenten sollte dem in der Organisation vorhandenen System zur Dokumentations-Kodierung entsprechen. Falls kein solches System vorhanden ist, kann diese Zeile gelöscht werden.

Änderungs-Historie

Datum	Version	Erstellt durch	Beschreibung der Änderung
	0.1	27001Academy	Erster Entwurf des Dokuments

Inhaltsverzeichnis

1. Zweck, Anwendungsbereich und Anwender

Der Zweck dieses Dokuments ist die Festlegung grundsätzlicher Vorschriften bei de rsicheren Entwicklung von Software und Systemen.

Dieses Dokument gilt für die Entwicklung und Wartung sämtlicher Dienstleistungen, Architektur, Software und Systeme, die Teil des Informationssicherheits-Managementsystems (ISMS) sind.

Anwender dieses Dokuments sind alle bei [Name der Organisation] in der Entwicklung und Wartung eingesetzten Mitarbeiter.

2. Referenzdokumente

- ISO/IEC 27001 Norm, Abschnitte A.14.1.2, A.14.1.3, A.14.2.1, A.14.2.2, A.14.2.4, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1
- Methodik zur Risikoeinschätzung und Risikobehandlung
- Sicherheitspolitik für Lieferanten
- [Richtlinie zum Änderungs-Management]/[Sicherheitsverfahren für die IT-Abteilung]
- Plan für Training und Awareness

Commented [27A4]: Wählen Sie, welches dieser beiden Dokumente Sie verwenden wollen.

3. Sichere Entwicklung und Wartung

Commented [27A5]: Da die verwendete Technik von Organisation zu Organisation unterschiedlich ist, müssen Sie diesen Abschnitt entsprechend Ihrer spezifischen Umstände anpassen.

3.1. Risikoeinschätzung beim Entwicklungsprozess

Zusätzlich zu der gemäß der Methodik zur Risikoeinschätzung und –Behandlung durchgeführten Risikoeinschätzung muss [Stellenbezeichnung] auch regelmäßig eine Einschätzung des folgenden durchführen:

Commented [27A6]: Falls nötig, spezxifizieren wie oft.

- Risiken im Zusammenhang mit unerlaubtem Zugang zum Entwicklungsumfeld
- [illegible]
- [illegible]
- [illegible]

3.2. Sicherung des Entwicklungsumfeldes

Commented [27A7]: Diesen Abschnitt löschen, falls Maßnahme A.14.2.6 als nicht anwendbar befunden wurde.

[Sowohl die internen als auch externen Anforderungen identifizieren; hier beschreiben, auf welche Weise der Zugang zum Entwicklungsumfeld ausschließlich für authorisierte Mitarbeiter beschränkt [illegible]

3.3. Sichere technische Prinzipien

Commented [27A8]: Diesen Abschnitt löschen, falls Maßnahme A.14.2.5 als nicht anwendbar befunden wurde.

[Stellenbezeichnung] verausgabt Verfahren für ein in technischer Hinsicht sicheres Informationssystem sowohl für die Entwicklung neuer Systeme als auch die Wartung bestehender Systeme, einschließlich der Festlegung der minimal einzuhaltenden Sicherheitsnormen.

[illegible]

3.4. Sicherheitsanforderungen

Im Fall der Beschaffung eines neuen Informationssystems oder der Weiterentwicklung oder Abänderung eines bereits bestehenden Systems muss [Stellenbezeichnung] die [illegible]

3.5. Sicherheitsanforderungen im Zusammenhang mit öffentlichen Netzwerken

[Stellenbezeichnung] ist verantwortlich für die Definierung der Sicherheitsmaßnahmen im Zusammenhang zu Informationen in Anwendungsdiensten, die über öffentliche Netzwerke laufen:

- Beschreibung der zu benutzenden Authentisierungssysteme
- [illegible]
- [illegible]

[Stellenbezeichnung] ist verantwortlich für die Festlegung der Maßnahmen für Online-Transaktionen, welche die mit einschließen müssen:

- Wie fehlerhaftes Routing verhindert wird
- Wie unvollständige Datenübertragung verhindert wird
- [illegible]
- [illegible]
- [illegible]

3.6. Prüfung und Testung der Umsetzung von Sicherheitsanforderungen

[Stellenbezeichnung] ist verantwortlich für die Festlegung der Methodik, Verantwortlichkeiten und [illegible]

3.7. Verwahrungsort

[Hier beschreiben, wo der Code und alle anderen Dateien, die sich auf Entwicklung beziehen, [illegible]

3.8. Verwaltung von Versionen

Commented [27A9]: z.B. Anleitung zu sicheren Programmiertechniken (separate für jede Programmiersprache), Benutzerauthentifizierung, sichere Session-Maßnahmen, Datumvalidierung, usw.

Alle architektonischen Ebenen abdecken – Geschäft, Daten, Anwendungen und Technologie.

Erfahren Sie hier mehr: What are secure engineering principles in ISO 27001:2013 control A.14.2.5? http://advisera.com/27001academy/blog/2015/08/31/what-are-secure-engineering-principles-in-iso-270012013-control-a-14-2-5/

Commented [27A10]: Diesen Abschnitt löschen, falls Maßnahme A.14.2.7 als nicht anwendbar befunden wurde.

Commented [27A11]: Diesen Abschnitt löschen, falls Maßnahme A.14.1.1 als nicht anwendbar befunden wurde.

Commented [27A12]: Um mehr über dieses Thema zu erfahren, lesen Sie bitte diesen Artikel:

How to set security requirements and test systems according to ISO 27001 https://advisera.com/27001academy/blog/2016/01/11/how-to-set-security-requirements-and-test-systems-according-to-iso-27001/

Commented [27A13]: Alternativ können Sie hier definieren, dass dies die Arbeitsaufgabe eines Projektteams ist u.ä.

Commented [27A14]: Diesen Abschnitt löschen, falls Maßnahmen A.14.1.2 und A.14.1.3 als nicht anwendbar befunden wurden.

Commented [27A15]: Maßnahmen können Digitalsignaturen, Verschlüsselung, Identifizierungs- und Authentisierungssysteme, usw. umfassen. Die Anwendung von Maßnahmen muss natürlich im Einklang mit Gesetzen und Vorschriften sein.

Commented [27A16]: Diesen Abschnitt löschen, falls Maßnahmen A.14.2.8 und A.14.2.9 als nicht anwendbar befunden wurden.

Commented [27A17]: z.B. Testeingaben und erwartete Outputs, Tools zur Code-Analyse oder Schwachstellen-Scanner.

[illegible]

Commented [27A18]: Gute Praxis ist es, die Tests sowohl vom eigenen Entwicklungs-Team als auch einem unabhängigen Team durchführen zu lassen.

Commented [27A19]: Nicht nur den abschließenden Test bei Beendigung eines Entwicklungsprojekts, aber auch im Verlauf des gesamten Entwicklungsprozesses.

[Hier definieren, welches System der Verwaltung von Versionen (Nummerierung, Datierung, usw.) eingesetzt wird und wie es in Ihrem Entwicklungsumfeld durchgesetzt wird]

3.9. Verwaltung von Änderungen

Änderungen bei der Entwicklung und während der Wartung der Systeme muss im Einklang mit [illegible] durchgeführt werden.

3.10. Schutz von Testdaten

Sowohl vertrauliche Daten als auch die persönlichen Daten von individuellen Personen dürfen nicht als Testdaten herangezogen werden. Ausnahmen können nur durch [Stellenbezeichnung] genehmigt [illegible] geschützt werden.

3.11. Erforderliches Sicherheitstraining

[Stellenbezeichnung] definiert die Stufe der Sicherheitsfertigkeiten und des Wissens, das im Rahmen des Entwicklungsprozesses erforderlich ist und schlägt die dafür erforderlichen Trainingskurse an [illegible] im Plan für Training und Awareness.

4. Verwaltung von Aufzeichnungen, die zu diesem Dokument erstellt wurden

Name der Aufzeichnung	Aufbewahrungsort	Verantwortlicher für Aufbewahrung	Maßnahmen zum Schutz der Aufzeichnungen	Aufbewahrungsdauer
[Liste der mit dem Entwicklungs-prozess in Zusammenhang stehenden Risiken]	Rechner von [Stellen-bezeichnung]	[Stellen-bezeichnung]	Nur [Stellen-bezeichnung] hat Zugang zu diesen Dateien	3 Jahre für ungültig gewordene Listen
[Verfahren für ein technisch sicheres Informations-system]	[Intranet der Organisation]	[Stellen-bezeichnung]	Nur [Stellen-bezeichnung] kann diese Dateien veröffentlichen und bearbeiten	3 Jahre für ungültig gewordene Verfahren
[Testpläne]	[Intranet der Organisation]	[Stellen-bezeichnung]	Nur [Stellen-bezeichnung]	3 Jahre für bereits durchgeführte Tests

Commented [27A20]: Diesen Abschnitt löschen, falls Maßnahmen A.14.2.2 und A.14.2.4 als nicht anwendbar befunden wurden.

Commented [27A21]: Um mehr über dieses Thema zu erfahren, lesen Sie bitte diesen Artikel:

How to manage changes in an ISMS according to ISO 27001 A.12.1.2 https://advisera.com/27001academy/blog/2015/09/14/how-to-manage-changes-in-an-isms-according-to-iso-27001-a-12-1-2/

Commented [27A22]: Wählen Sie, welches dieser beiden Dokumente Sie verwenden wollen.

Commented [27A23]: Diesen Abschnitt löschen, falls Maßnahme A.14.3.1 als nicht anwendbar befunden wurde.

Commented [27A25]: Die Aufbewahrungsdauer Ihren spezifischen Bedürfnissen anpassen.

Commented [27A24]: Bitte ändern Sie diese Aufzeichnungen derart, dass sie zu denen passen, die Sie bereits in Ihrem Unternehmen haben. Sollten Sie keine ähnlichen Aufzeichnungen haben, können Sie neue Aufzeichnungen in einem neuen Format erstellen, welches Ihnen am besten zusagt.

			kann diese Dateien veröffentlichen und bearbeiten	

5. Gültigkeit und Dokumenten-Handhabung

Dieses Dokument ist gültig ab [Datum].

[illegible]

Commented [27A26]: Dies ist lediglich eine Empfehlung; Häufigkeit nach Bedarf anpassen.

Für die Auswertung des Dokuments auf Wirksamkeit und Angemessenheit müssen folgende Kriterien berücksichtigt werden:

- [illegible]

6. Anhänge

- Anhang 1 – Spezifikation der Sicherheitsanforderungen

[Stellenbezeichnung]
[Name]

_____
[Unterschrift]

Commented [27A27]: Nur notwendig, falls das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen das Unterschreiben von Papierdokumenten vorschreibt.